KI for cybersikkerhet & cybersikkerhet for KI

Sponset av Gemini-senter for Pålitelig og Bærekraftig AI og prosjektet AI&CYBER
www.sintef.no/geminai

Gencer Erdogan, Seniorforsker
SINTEF Digital

Forum, Forskningsparken
24. oktober 2024

Hvorfor er dette et viktig tema for samfunnet?

Forventer sterk vekst i cyberangrep drevet av AI i 2024

Cybersikkerhetsselskapet Trend Micro retter en kraftig advarsel mot de transformative og potensielt farlige implikasjonene av generativ kunstig intelligens (GenAI) i cybersikkerhetslandskapet.

Kunstig intelligens kan øke svindel og dataangrep

– Fører ofte til tap i millionklassen

IT-angrep fra Russland, Iran, Kina og organiserte kriminelle rammer også «vanlige» bedrifter. – De færreste har regnet på hva det koster å bli rammet, advarer Advania.

I 2024 vil kunstig intelligens være både mål og virkemiddel for cyberangrep

Posten-sjefen om cybertrusler: – Må være forberedt

Vi står overfor ein aukande trussel for cyberangrep i åra som kjem. (Illustrasjonsfoto: Colourbox)

Stadig større sjanse for å bli angripen i cyberspace

Professor i cybertryggleik trur fleire og fleire vestlege land vil endra strategi og ikkje berre forsvara seg mot angrep frå andre.

Dramatisk økning i cyberangrep: – Flere og mer alvorlige hendelser

NSM la fredag fram rapporten «Nasjonalt digitalt risikobilde 2023».

Hvordan kan KI styrke cybersikkerhet, og hvordan kan vi sikre KI-systemene?

KI for Cybersikkerhet

- **Trusseldeteksjon**: KI kan analysere store mengder data for å identifisere mistenkelige mønstre og oppdage cybertrusler.
- **Automatisering**: KI kan automatisere sikkerhetsoppgaver som overvåking og respons.
- **Prediktiv analyse**: KI kan forutsi fremtidige angrep basert på historiske data og trender.

Cybersikkerhet for KI

- **Datasikkerhet**: Beskytte treningsdata mot manipulering for å sikre at KI-systemer ikke blir villedet.
- **Modellintegritet**: Sikre at KI-modeller ikke blir kompromittert av ondsinnede aktører som kan endre modellens atferd.
- **Personvern**: Implementere tiltak for å beskytte sensitiv informasjon som KI-systemer behandler.

Program

10:00 – 10:10	Velkomst – Gencer Erdogan (SINTEF)
10:10 – 10:55	KI og cybersikkerhet – Audun Jøsang (Universitetet i Oslo)
10:55 – 11:40	Onde Nevrale Nettverk – Michael Alexander Riegler (Simula)
11:40 – 12:25	Lunsj
12:25 – 13:10	KI i cybersikkerhet: Derfor er ‘sec’ i DevSecOps viktigere enn noensinne i dagens forretningslandskap! – Kamer Vishi (Kommunalbanken)
13:10 – 13:55	KI-drevet sikkerhetsorkestrering, automatisering og respons for digitale tvillingbaserte kritiske systemer – Phu Nguyen (SINTEF)
13:55 – 14:00	Oppsummering og slutt - Gencer Erdogan (SINTEF)

SINTEF

Teknologi for et bedre samfunn